From Local to Robust Testing via Agreement Testing

Irit Dinur[1]
Department of Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel
irit.dinur@weizmann.ac.il

Prahladh Harsha[2]
Tata Institute of Fundamental Research, India
prahladh@tifr.res.in

Tali Kaufman
Department of Computer Science, Bar-Ilan University, Ramat Gan, Israel
kaufmant@mit.edu

Noga Ron-Zewi
Department of Computer Science, University of Haifa, Haifa, Israel
noga@cs.haifa.ac.il

Abstract

A local tester for an error-correcting code is a probabilistic procedure that queries a small subset of coordinates, accepts codewords with probability one, and rejects non-codewords with probability proportional to their distance from the code. The local tester is *robust* if for non-codewords it satisfies the stronger property that the average distance of local views from accepting views is proportional to the distance from the code. Robust testing is an important component in constructions of locally testable codes and probabilistically checkable proofs as it allows for composition of local tests.

In this work we show that for certain codes, any (natural) local tester can be converted to a roubst tester with roughly the same number of queries. Our result holds for the class of *affine-invariant lifted codes* which is a broad class of codes that includes Reed-Muller codes, as well as recent constructions of high-rate locally testable codes (Guo, Kopparty, and Sudan, ITCS 2013). Instantiating this with known local testing results for lifted codes gives a more direct proof that improves some of the parameters of the main result of Guo, Haramaty, and Sudan (FOCS 2015), showing robustness of lifted codes.

To obtain the above transformation we relate the notions of local testing and robust testing to the notion of *agreement testing* that attempts to find out whether valid partial assignments can be stitched together to a global codeword. We first show that agreement testing implies robust testing, and then show that local testing implies agreement testing. Our proof is combinatorial, and is based on expansion / sampling properties of the collection of local views of local testers. Thus, it immediately applies to local testers of lifted codes that query random affine subspaces in $\mathbb{F}_q^m$, and moreover seems amenable to extension to other families of locally testable codes with expanding families of local views.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography

[1] Supported by ERC-CoG grant number 772839.
[2] Research supported in part by the UGC-ISF grant and the Swarnajayanti Fellowship. Part of the work was done when the author was visiting the Weizmann Institute of Science.

10th Innovations in Theoretical Computer Science (ITCS 2019).
Editor: Avrim Blum; Article No. 29; pp. 29:1–29:18

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Keywords and phrases Local testing, Robust testing, Agreement testing, Affine-invariant codes, Lifted codes

Digital Object Identifier 10.4230/LIPIcs.ITCS.2019.29

1 Introduction

Our main result shows a transformation from *local testing* to *robust testing* for the class of *affine-invariant lifted codes*. We start by describing the notions of local testing, robust testing, and lifted codes.

1.1 Local testing and robust testing

A code is a subset $C \subseteq \Sigma^n$. The elements of C are called *codewords*, Σ is the *alphabet* of the code, and n is the *block length*. The *rate* of the code is the ratio $(\log_{|\Sigma|} |C|)/n$. The code is *linear* if $\Sigma = \mathbb{F}_q$ where $\mathbb{F}_q$ is the finite field of q elements, and C is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. It will be convenient to think of codewords in C as functions $f : U \to \Sigma$ where U is a domain of size n. For a pair of functions $f, g : U \to \Sigma$ we let $\mathrm{dist}(f, g)$ denote the fraction of inputs $x \in U$ for which $f(x) \neq g(x)$. The *relative distance* $\mathrm{dist}(C)$ of the code is the minimum of $\mathrm{dist}(f, g)$ over all codewords $f, g \in C$. For a function $f : U \to \Sigma$ we let $\mathrm{dist}(f, C)$ denote the minimum of $\mathrm{dist}(f, g)$ over all codewords $g \in C$.

A *local tester* for the code C is a probabilistic oracle algorithm that on oracle access to a function $f : U \to \Sigma$ makes at most Q queries to f, and accepts $f \in C$ with probability one, while rejecting $f \notin C$ with probability at least $\alpha \cdot \mathrm{dist}(f, C)$. We refer to Q as the *query complexity* of the tester, and to α as the *soundness*. In this work we shall restrict our attention to local testers that pick a random subset $K \subseteq U$ of cardinality Q according to some distribution, and accept if and only if $f|_K \in C|_K$.[3] The requirement then is that $f|_K \in C|_K$ with probability one whenever $f \in C$, and

$$\Pr_K[f|_K \notin C|_K] \geq \alpha \cdot \mathrm{dist}(f, C) \tag{1}$$

otherwise.

In this work we will be interested in the stronger notion of robustness. We say that a local tester as above is *robust* if for non-codewords the average distance of its local views from accepting views is proportional to the distance of the given function from the code. That is, as before we require that $f|_K \in C|_K$ with probability one whenever $f \in C$, but instead of (1) we now require that

$$\mathbb{E}_K\big[\mathrm{dist}(f|_K, C|_K)\big] \geq \alpha \cdot \mathrm{dist}(f, C) \tag{2}$$

whenever $f \notin C$. Here we refer to α as the *robustness* of the tester.

The notion of robustness was introduced by Ben-Sasson and Sudan [8] based on analogous notions for probabilistically checkable proofs [5, 15]. Robustness is a natural property of local testers that relates the global distance of a function from the code to its local distance from accepting views on local views. Moreover, robustness is also an important ingredient in constructions of locally testable codes and probabilistically checkable proofs as it allows for composition of local tests. Specifically, it follows by definition that if a code C is robustly

[3] Local testers may generally apply a more complex predicate on $f|_K$. However, natural local testers are typically of the restricted form we consider, and moreover it can be shown that a local tester for a linear code must be of this form [6].

testable with query complexity Q and soundness α, and additionally each local restriction $C|_K$ is locally testable with query complexity Q' and soundness α', then the code C is locally testable with query complexity Q' and soundness $\alpha \cdot \alpha'$. This property is useful when local restrictions can be tested efficiently which can happen if the code has many symmetries (as is the case with the class of lifted codes considered in this work) or can be achieved, in the case of probabilistically checkable proof, by attaching a short proof of proximity.

One can easily observe that (2) implies (1) since $f|_K \notin C|_K$ whenever $\mathrm{dist}(f|_K, C|_K) > 0$, so robustness is a stronger requirement than local testing. For the other direction, note that a local tester with soundness α has robustness at least α/Q since $\mathrm{dist}(f|_K, C|_K) \geq 1/Q$ whenever $f|_K \notin C|_K$. A natural question is whether this loss in roubstness is necessary, and whether robustness is strictly stronger notion than local testing. In this work we shall show that this loss is unnecessary for the class of lifted codes, discussed below.

1.2 Lifted codes

Lifted codes are specified by a *base code* $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ and a dimension $m \geq \ell$. We further assume that the base code C is linear and *affine-invariant*, that is, for any codeword $f \in C$, and for any affine transformation $A : \mathbb{F}_q^\ell \to \mathbb{F}_q^\ell$ it holds that $f \circ A \in C$. Given these we define the *lifted code* $C^{\ell \nearrow m}$ to be the code consisting of all functions $f : \mathbb{F}_q^m \to \mathbb{F}_q$ that satisfy that $f|_L \in C$ for any ℓ-dimensional affine subspace L.

Lifted codes were first introduced by Ben-Sasson et al [7], and their local testability properties were further explored in subsequent work [20, 21, 19]. They are a natural generalization of the well-studied family of Reed-Muller codes, and moreover they also give rise to new families of locally testable codes that outperform Reed-Muller codes in certain range of parameters [20]. Specifically, lifted codes lead to one of the two known constructions (the other one being tensor codes [8, 9, 27, 24]) of high-rate locally testable codes (i.e., locally testable codes with rate approaching one and sublinear locality). Generally, lifted codes form a natural subclass of affine-invariant codes satisfying the "single-orbit characterization" property that is known to imply local testability, as well as local decodability [23].

There is a natural local test associated with lifted codes: on oracle access to a function $f : \mathbb{F}_q^m \to \mathbb{F}_q$, pick a uniform random ℓ-dimensional affine subspace L and accept if and only if $f|_L \in C$. It follows immediately by definition that this test accepts any valid codeword $f \in C^{\ell \nearrow m}$ with probability one, but more work is required to show that this test is sound. Specifically, since the test forms a single orbit characterization, it follows from [23] that it has soundness roughly $q^{-2\ell}$. The dependence of the soundness on the dimension ℓ was later eliminated in [21] who showed soundness that is only a function of q (though an extremely quickly decaying one).

As for robustness, the above local testing results, together with the straightforward transformation from local testing to robust testing, immediately give robustness that is dependent on the dimension ℓ. This was eliminated recently in [19] who showed robustness of the form $\mathrm{poly}(\delta)$ (about δ^{74}, where δ is the relative distance of the code) for the local test that queries subspaces of slightly larger dimension of 2ℓ. Interestingly, [19] did not rely on the aforementioned local testing results, but rather relied on viewing lifted codes as the intersection of "modified tensor codes". They then proceeded by showing that these modified tensor codes are robustly testable (using the proof method of [27] showing robustness of tensor codes), and that this implies local testability of the lifted code (see Section 2.4 for more details about the proof method of [19]).

1.3 Our results

Our main result gives a transformation from local testing to robust testing, that does not suffer the factor of Q (the query complexity) loss in robustness, for the class of lifted codes. The transformation uses local testability in a "black-box" manner, and shows that if a code in this family is locally testable (using the natural subspace tester) then it is also robustly testable with roughly the same number of queries and robustness.

For $k \geq \ell$, let the *k-dimensional (subspace) test* denote the local tester that on oracle access to a function $f : \mathbb{F}_q^m \to \mathbb{F}_q$ queries a uniform random k-dimensional affine subspace K and accepts if and only if $f|_K \in C^{\ell \nearrow k}$.

▶ **Theorem 1** (Main). *Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq k \geq \ell$. Suppose that $C^{\ell \nearrow m}$ is locally testable using the k-dimensional test with query complexity q^k and soundness α, and let $\delta := \min_{k \leq r \leq m} \mathrm{dist}(C^{\ell \nearrow r})$. Then $C^{\ell \nearrow m}$ is robustly testable using the $(2k + \log_q(4/\delta))$-dimensional test with query complexity $O(q^{2k}/\delta)$ and robustness $\Omega(\alpha \cdot \delta^3)$.*

Note that if the relative distance δ is constant, we only incur a constant multiplicative loss in robustness and testing dimension.

To apply the above theorem one can instantiate it with the local testing result of [23] that says that lifted codes are locally testable using the ℓ-dimensional test with soundness $\approx q^{-2\ell}$ (see Theorem 6 below). However, to obtain constant robustness we need that the soundness of the initial local tester would be constant (independent of q and ℓ), and for this we observe (in Proposition 19) that the soundness of [23] can be easily amplified to $\Omega(1)$ at the cost of increasing the testing dimension to $\approx 3\ell$.[4] Using this observation we obtain the following.

▶ **Corollary 2.** *Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code of relative distance δ, and $m \geq \ell$. Then $C^{\ell \nearrow m}$ is robustly testable using the $(6\ell + \log_q(128/\delta))$-dimensional test with robustness $\Omega(\delta^3)$.*

Compared to the above corollary, [19] use lower dimension of 2ℓ, but also obtain lower soundness of $\Omega(\delta^{74})$.

As described next, our proof is combinatorial, relying mainly on expansion / sampling properties of the collection of local views. In particular, it uses very little about the algebraic structure of lifted codes or the base code. We thus hope that such techniques would prove useful in the future for showing robustness for other families of locally testable codes with similar expansion properties.

2 Proof overview

Our proof is based on a new connection between the notions of local testing, robust testing, and *agreement testing*. Specifically, we show that for the class of lifted codes agreement testing implies robust testing, and local testing implies agreement testing. The combination of these two implications gives our main Theorem 1. Next we elaborate on the notion of agreement testing, followed by an overview of each of the implications.

[4] Such an amplification with similar blow-up in query complexity can be easily obtained by repeating the test and accepting if and only if all invocations accept; we however need that the tester would be a subspace tester which can be obtained using sampling properties of affine subspaces.

2.1 Agreement testing

An *agreement test* attempts to find out whether partial assignments to local views can be stitched together to a single global codeword. Let $C \subseteq \{U \to \Sigma\}$ be a code, and let $\mathcal{S}$ be a collection of subsets of U. An *agreement tester* for $C, \mathcal{S}$ is a probabilistic oracle algorithm that receives oracle access to a collection of partial assignments $\{f_S : S \to \Sigma \mid S \in \mathcal{S}\}$ on sets of $\mathcal{S}$, where $f_S \in C|_S$ for any $S \in \mathcal{S}$. The tester queries a few of the f_S's, and is required to accept with probability one any collection $(f_S)_S$ that is consistent with some global codeword $g \in C$ (that is, $g|_S = f_S$ for any $S \in \mathcal{S}$), while rejecting any inconsistent collection $(f_S)_S$ with probability proportional to the minimal fraction of f_S's that must be changed in order to be consistent with some global codeword. In this work we focus on the two query agreement tester that picks a pair of sets $S, S' \in \mathcal{S}$ according to some distribution and accepts if and only if f_S and $f_{S'}$ agree on their intersection $S \cap S'$.

Agreement testing has first appeared in PCP constructions [3, 2] as so-called "low degree tests", and is a key component in the proof of almost all PCP theorems. A prime example is the line vs. line low degree test [17, 26] in the proof of the PCP theorem. In the PCP construction, a function on a large vector space is replaced by an ensemble of (supposed) restrictions to all possible affine lines. These restrictions are supplied by a prover and are not a priori guaranteed to agree with any single global function. The "low degree test" is run by the verifier to check that restrictions on intersecting lines agree with each other, i.e. they give the same value to the point of intersection. The main point of the argument is to show that the passing of the test implies agreement with a single global function. In these early low degree tests (including the linearity testing work of [10]) an agreement test component can be discerned but quite implicitly. Indeed, it was only separated in the works [25, 4] that looked at the so-called list-decoding regime[5], with the goal of proving a large gap for the PCP.

Goldreich and Safra [18] tried to separate the algebraic aspect of the low degree test from the combinatorial, and formulated a more general "consistency test" which is also referred to as an agreement test. They also proved a certain local to global result which was too weak to be useful for PCPs. In hindsight it is clear that since their family of subsets consisted of axis parallel lines, the expansion was not strong enough for a good agreement test. Only recently [13] the role of expansion underlying the family of subsets had begun to be uncovered.

Work on agreement testing then continued the combinatorial direction of [18] mainly in the list-decoding regime for direct product testing [15, 12, 22, 16, 14]. The techniques developed in this line of work turn out to be useful also for agreement testing in the unique-decoding regime (which is the more standard testing regime), and in particular for our work here.

2.2 Agreement testing implies robust testing

We begin with an overview of the simpler implication from agreement testing to robust testing. Suppose that we have a two query agreement tester for $C, \mathcal{S}$ as described above. We would like to show that the local tester that queries a random $S \in \mathcal{S}$ is robust. Let $\mathcal{T}$ be the collection of subsets of U formed by pairwise intersections of sets in $\mathcal{S}$. The main properties we need out of $\mathcal{S}, \mathcal{T}$ are sampling properties, specifically, that $\mathcal{S}$ samples well the set of points U, and that for any $S \in \mathcal{S}$ all sets in $\mathcal{T}$ contained in S sample well the set of points in S. The main property we need out of the code is that its restrictions to sets in $\mathcal{T}$

[5] In the list decoding regime one would like to reject a function that is $(1-\epsilon)$-far from the code with very high-probability of $1 - O(\epsilon)$.

have distance. In the case of lifted codes these properties can be guaranteed by letting $\mathcal{S}, \mathcal{T}$ be families of affine subspaces of fixed dimension.

To see that the proposed local tester is indeed robust, suppose that we have a function $f : U \to \Sigma$ that is close to $C|_S$ on a typical S, our goal is to show that f is close to a codeword $g \in C$. We first create an instance $(f_S)_S$ for the agreement tester by letting $f_S \in C|_S$ be the closest valid assignment to $f|_S$. Next observe that since $f|_S$ is typically close to f_S, and by assumption that T's sample well inside S's, for a typical T and S, S' containing T it holds that $f_S|_T \approx f|_T \approx f_{S'}|_T$, and by distance property on $\mathcal{T}$ this implies in turn that typically $f_S|_T = f_{S'}|_T$. Consequently, agreement testability implies the existence of a codeword $g \in C$ that agrees with most f_S, and so $g|_S = f_S \approx f|_S$ for most S. But since $\mathcal{S}$ samples well inside U we conclude that f must be close to g as required.

2.3 Local testing implies agreement testing

We now turn to the local testing to agreement testing implication which is a bit more involved. Suppose that we have a local testing algorithm for C that queries a random set $K \in \mathcal{K}$ and accepts if and only if $f|_K \in C|_K$. We would like to obtain an agreement tester for C with respect to some collection of subsets $\mathcal{S}$. As before, let $\mathcal{T}$ be the collection of subsets of U formed by pairwise intersections of sets in $\mathcal{S}$. Once more the main properties we require out of $\mathcal{S}, \mathcal{T}, \mathcal{K}$ are sampling properties. Specifically, we need that $\mathcal{S}$ samples well inside U, and that for any $T \in \mathcal{T}$ all sets in $\mathcal{K}$ contained in T sample well inside T. We also require distance properties out of C, specifically that C has distance on U and on restrictions to sets in $\mathcal{S}$ and $\mathcal{T}$. Once more, in the case of lifted codes these properties can be guaranteed by letting $\mathcal{S}, \mathcal{T}, \mathcal{K}$ be families of affine subspaces of fixed dimension.

To show agreement testability, let $(f_S)_S$ be a collection of valid assignments to sets in $\mathcal{S}$ (so $f_S \in C|_S$ for any S), and suppose that f_S agrees with $f_{S'}$ on $S \cap S'$ for most pairs S, S'. Our goal will be to find a global codeword $g \in C$ that agrees with most f_S. We find the function g in the following three stages.

Initial stage

In the first stage we define for any $K \in \mathcal{K}$ a "most popular function" Plur_K by choosing the most common value among $f_S|_K$ going over all $S \in \mathcal{S}$ containing K. We then show, using the assumption that f_S's typically agree on their intersections, that this most popular function is obtained with overwhelming probability for a typical K.

Local structure stage

In the second stage we define for each $K \in \mathcal{K}$ a function $g_K : U \to \Sigma$ by letting $g_K(x)$ be the most common "vote" among all f_S that contain K and x and agree with Plur_K on K (this function is well defined because of the initial stage). We then show that for a typical K, g_K is close to some function $h_K \in C$, and moreover $h_K|_S = f_S$ for most S containing K.

To see why the above holds, first note that by assumptions that C has distance on T's, and K's sample well inside T's, if a pair of f_S's agree on K then they must typically also agree on their whole intersection. Therefore $g_K(x)$ is also typically defined with overwhelming probability. Consequently, for a typical K, and most K', $g_K|_{K'}$ agrees with some f_S. Recalling that f_S's are valid assignments, local testability then implies the existence of $h_K \in C$ that is close to g_K. The fact that $h_K|_S = f_S$ for most S containing K follows by assumption that $\mathcal{S}$ samples well U, and distance property on $\mathcal{S}$.

Global structure stage

In the final stage we show that there exists $\hat{K}$ such that $h_{\hat{K}}$ agrees with f_S for most S (not necessarily containing $\hat{K}$). We can then set our "global function" g to be equal to $h_{\hat{K}}$. To this end, we first observe that it suffices to show that most functions h_K are in fact identical. This now follows since for typical $S \supseteq K \cup K'$ it holds that $h_K|_S = f_S = h_{K'}|_S$, and consequently since $\mathcal{S}$ samples U it must typically hold that $h_K = h_{K'}$.

2.4 The proof method of Guo et al

The proof method of Guo et al [19] for showing robustness of lifted codes is very different from ours. In particular, it relies heavily on the algebraic structure of lifted codes. More specifically, the proof is based on viewing the lifted codes as the intersection of "modified tensor codes". The *tensor product* $C^{\otimes m}$ of a code $C \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ can be thought of as the 'axis-parallel lifting' of C, that is, it is the code that consists of all functions $f : \mathbb{F}_q^m \to \mathbb{F}_q$ whose restrictions to any axis-parallel line belong to C. The "modified tensor code" is a code of the form $C_b^{\otimes m}$ where b is a direction in $\mathbb{F}_q^m$, and $C_b^{\otimes m}$ consists of all functions $f \in C^{\otimes m}$ whose restrictions to lines in direction b also belong to C.

The authors first use the proof method of [27], showing robust testing of tensor codes, to show that the modified tensor codes are also robustly testable. They then use the fact that the lifted code is the intersection of all codes of the form $C_b^{\otimes m}$ for all directions b (this is true when the dimension of the base code for lifting is $\ell = 1$; when $\ell > 1$ the proof becomes more complicated) to deduce robust testability for the lifted code. However, since intersection of robustly testable codes is not necessarily robustly testable, a non-trivial work is required to show robust testability, which in particular exploits the degree structure of affine-invariant lifted codes.

The above program can be carried out only when the dimension m of the lifted code is a small constant multiple of ℓ, and the authors use the "bootstrapping" technique [26, 2, 4, 1] to extend the result to work for arbitrary large m.

In contrast, we work directly with lifted codes of large dimension which allows us to exploit the sampling / expansion properties of large affine subspaces in $\mathbb{F}_q^m$. To the best of our knowledge, even for the special case of low-degree polynomials, this gives the first analysis of robustness that is not based on the two step approach of first analyzing the constant dimensional case and only then moving to the general dimensional case.

As opposed to [19] who reprove local testability on the way, our proof uses local testability in a black-box manner. Thus, it exhibits a separation between the algebraic properties that are used for showing local testability, and the combinatorial properties that are needed in order to turn local testability into robust testability.

Paper organization

The rest of the paper is organized as follows. In Section 3 we set some notation, provide some definitions, and present the expansion properties of subspaces that we use. The transformation from agreement testing to robust testing is given in Section 4, while the transformation from local testing to agreement testing apperas in Section 5. We wrap-up in Section 6 with the full transformation from local testing to robust testing that proves our main Theorem 1 and Corollary 2.

3 Preliminaries

For a prime power q, let $\mathbb{F}_q$ denote the finite field of q elements. Let $\{\mathbb{F}_q^m \to \mathbb{F}_q\}$ denote the set of functions mapping $\mathbb{F}_q^m$ to $\mathbb{F}_q$. In what follows we focus on codes which are subsets of functions $C \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$. For a pair of functions $f, g : \mathbb{F}_q^m \to \mathbb{F}_q$ we use $\mathrm{dist}(f, g)$ to denote the fraction of inputs $x \in \mathbb{F}_q^m$ for which $f(x) \neq g(x)$. The *relative distance* $\mathrm{dist}(C)$ of the code C is $\min_{f \neq g \in C}\{\mathrm{dist}(f, g)\}$. For a function $f : \mathbb{F}_q^m \to \mathbb{F}_q$ we use $\mathrm{dist}(f, C)$ to denote $\min_{g \in C}\{\mathrm{dist}(f, g)\}$.

The code C is said to be *linear* if it is an $\mathbb{F}_q$-linear subspace, i.e., for every $\alpha \in \mathbb{F}_q$ and $f, g \in C$, we have $\alpha f + g \in C$. A function $A : \mathbb{F}_q^m \to \mathbb{F}_q^m$ is said to be an *affine transformation* if there exist a matrix $M \in \mathbb{F}_q^{m \times m}$ and a vector $b \in \mathbb{F}_q^m$ such that $A(x) = Mx + b$. The code C is said to be *affine-invariant* if for every affine transformation A and every $f \in C$ we have $f \circ A \in C$ (where $(f \circ A)(x) = f(A(x))$).

3.1 Lifted codes

A subset $L \subseteq \mathbb{F}_q^m$ is said to be an *ℓ-dimensional affine subspace* if there exist $\alpha_0 \in \mathbb{F}_q^m$ and linearly independent $\alpha_1, \ldots, \alpha_\ell \in \mathbb{F}_q^m$ such that $L = \{\alpha_0 + \sum_{i=1}^{\ell} \alpha_i x_i | x_1, \ldots, x_\ell \in \mathbb{F}_q\}$. We fix an arbitrary affine map $\gamma_L : \mathbb{F}_q^\ell \to L$ (which we can view as a parameterization of L). For a function $f : \mathbb{F}_q^m \to \mathbb{F}_q$, the restriction $f|_L$ is viewed as a function in $\{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ through $f \circ \gamma_L : \mathbb{F}_q^\ell \to \mathbb{F}_q$. In particular, when we ask if $f|_L \stackrel{?}{\in} C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ what we are really asking is whether $f \circ \gamma_L \in C$. Note that if C is affine-invariant, whether $f|_L \in C$ does not depend on the choice of the parametrization γ_L.

▶ **Definition 3** (Lifted codes). Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq \ell$. The *m-dimensional lift* $C^{\ell \nearrow m}$ of C is given by

$$C^{\ell \nearrow m} := \left\{f : \mathbb{F}_q^m \to \mathbb{F}_q \mid f|_L \in C \text{ for every } \ell\text{-dimensional affine subspace } L \subseteq \mathbb{F}_q^m\right\}.$$

▶ **Proposition 4** (Distance of lifted codes, [20], Theorem 5.1, Part (2)). *Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq \ell$. Then* $\mathrm{dist}(C^{\ell \nearrow m}) \geq \mathrm{dist}(C) - q^{-\ell}$.

3.2 Local testing, robust testing, and agreement testing

We now formally define the notions of local testing, robust testing, and agreement testing, specialized to the class of lifted codes and subspace testers. In the case of local testing and robust testing this simply means that the tester samples a uniform random k-dimensional affine subspace and its accepting views are codewords in $C^{\ell \nearrow k}$.

▶ **Definition 5** (Local testing of lifted codes). Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq k \geq \ell$. The m-dimensional lift $C^{\ell \nearrow m}$ is *(k, α)-testable* if for every $f : \mathbb{F}_q^m \to \mathbb{F}_q$ it holds that

$$\Pr_K\left[f|_K \notin C^{\ell \nearrow k}\right] \geq \alpha \cdot \mathrm{dist}(f, C^{\ell \nearrow m}),$$

where the probability is over a uniform random k-dimensional affine subspace $K \subseteq \mathbb{F}_q^m$.

▶ **Theorem 6** ([23], Theorem 2.9). *Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq \ell$. Then the ℓ-dimensional test rejects a function $f : \mathbb{F}_q^m \to \mathbb{F}_q$ with probability at least $\frac{1}{2} \cdot \min\left\{q^{-2\ell}, \mathrm{dist}(f, C^{\ell \nearrow m})\right\}$. In particular, $C^{\ell \nearrow m}$ is $\left(\ell, \frac{q^{-2\ell}}{2}\right)$-testable.*

▶ **Definition 7** (Robust testing of lifted codes). Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq k \geq \ell$. The m-dimensional lift $C^{\ell \nearrow m}$ is (k, α)-*robust* if for every $f : \mathbb{F}_q^m \to \mathbb{F}_q$ it holds that

$$\mathbb{E}_K \left[\mathrm{dist}(f|_K, C^{\ell \nearrow k}) \right] \geq \alpha \cdot \mathrm{dist}(f, C^{\ell \nearrow m}),$$

where the expectation is over a uniform random k-dimensional affine subspace $K \subseteq \mathbb{F}_q^m$.

We note the following easy implications.

▶ **Proposition 8.** *Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq k \geq \ell$. Then the following hold.*

1. *If $C^{\ell \nearrow m}$ is (k, α)-robust then it is (k, α)-testable.*
2. *If $C^{\ell \nearrow m}$ is (k, α)-testable then it is $(k, \alpha \cdot q^{-k})$-robust.*
3. *If $C^{\ell \nearrow m}$ is (k, α)-testable then it is (r, α)-testable for any $k \leq r \leq m$.*
4. *If $C^{\ell \nearrow m}$ is (k, α)-robust then it is (r, α)-robust for any $k \leq r \leq m$.*

Proof. Part (1) follows since $f|_K \notin C^{\ell \nearrow k}$ whenever $\mathrm{dist}(f|_K, C^{\ell \nearrow k}) > 0$, while Part (2) follows since $\mathrm{dist}(f|_K, C^{\ell \nearrow k}) \geq q^{-k}$ whenever $f|_K \notin C^{\ell \nearrow k}$.

Part (3) follows by observing that for a uniform random r-dimensional affine subspace R,

$$\begin{aligned} \Pr_R \left[f|_R \notin C^{\ell \nearrow r} \right] &= \mathbb{E}_R \left[\mathbb{1}_{f|_R \notin C^{\ell \nearrow r}} \right] \\ &\geq \mathbb{E}_R \left[\Pr_{K \subseteq R} \left[f|_K \notin C^{\ell \nearrow k} \right] \right] \\ &= \Pr_K \left[f|_K \notin C^{\ell \nearrow k} \right], \end{aligned}$$

where the inequality follows since $f|_R \in C^{\ell \nearrow r}$ implies that $f|_K \in C^{\ell \nearrow k}$ for any K.

Finally, Part (4) follows by letting f_R be the codeword in $C^{\ell \nearrow r}$ that is closest to $f|_R$, and noting that

$$\begin{aligned} \mathbb{E}_R \left[\mathrm{dist}(f|_R, C^{\ell \nearrow r}) \right] &= \mathbb{E}_R \left[\mathrm{dist}(f|_R, f_R) \right] \\ &= \mathbb{E}_R \left[\mathbb{E}_{K \subseteq R} \left[\mathrm{dist}(f|_K, f_R|_K) \right] \right] \\ &\geq \mathbb{E}_R \left[\mathbb{E}_{K \subseteq R} \left[\mathrm{dist}(f|_K, C^{\ell \nearrow k}) \right] \right] \\ &= \mathbb{E}_K \left[\mathrm{dist}(f|_K, C^{\ell \nearrow k}) \right], \end{aligned}$$

where the inequality follows since $f_R|_K \in C^{\ell \nearrow k}$ for any K. ◀

We now turn to the definition of agreement testing. The agreement testers we consider are two query testers that for $t < s$, sample a uniform random t-dimensional affine subspace T, and a pair of uniform random s-dimensional affine subspaces S, S' containing T, and accept if and only if $f_S, f_{S'}$ agree on T.

For a code $C \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ we let $C(s)$ be the code containing all collections $(f_S)_S$ of partial assignments to s-dimensional affine subspaces that are consistent with some global codeword $g \in C$, formally,

$$C(s) := \left\{ (f_S)_S \mid \exists\, g \in C \text{ such that } g|_S = f_S \text{ for any } s\text{-dimensional affine subspace } S \right\}.$$

For a pair of collections $(f_S)_S, (g_S)_S$ of partial assignments to s-dimensional affine subspaces we denote by $\mathrm{dist}((f_S)_S, (g_S)_S)$ the fraction of s-dimensional affine subspaces S for which $f_S \neq g_S$, and we define $\mathrm{dist}((f_S)_S, C(s))$ accordingly.

▶ **Definition 9** (Agreement testing of lifted codes)**.** Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq s > t \geq \ell$. The m-dimensional lift $C^{\ell \nearrow m}$ is (s,t,α)-*agreement testable* if for every collection $(f_S)_S$ where $f_S \in C^{\ell \nearrow s}$ for every s-dimensional affine subspace S it holds that

$$\Pr_{T,\, S \supseteq T,\, S' \supseteq T}[f_S|_T \neq f_{S'}|_T] \geq \alpha \cdot \mathrm{dist}\big((f_S)_S, C^{\ell \nearrow m}(s)\big),$$

where the probability is over a uniform random t-dimensional affine subspace $T \subseteq \mathbb{F}_q^m$, and uniform random s-dimensional affine subspaces S, S' containing T.

3.3 Subspace expansion

Let $d_0, d_1, d_2 \in \{0, 1, \ldots, m\}$ be integers, and let $W \subseteq \mathbb{F}_q^m$ be a fixed affine subspace of dimension d_0. We denote by $\mathcal{I}_{d_1,d_2}(d_0)$ the bipartite graph whose left side are all d_1-dimensional affine subspaces of $\mathbb{F}_q^m$, whose right side are all d_2-dimensional affine subspaces of $\mathbb{F}_q^m$ containing W, and an edge (U,V) is present in the graph if and only if $U \subseteq V$ (note that the structure of the graph is independent of the choice of W). Our proof makes use of expansion properties of this graph.

▶ **Proposition 10.** *The second largest normalized singular value of the adjacency matrix of $\mathcal{I}_{d_1,d_2}(d_0)$ is at most $q^{-(d_2-d_1-d_0)/2}$.*

Proof. Let $\mathrm{Gr}(\mathrm{m}, \mathrm{d}_1)$ be the Grassmann graph whose vertices are d_1-dimensional spaces and edges connect two d_1-spaces that intersect on an $d_1 - 1$ space. We quote [11, Theorem 9.3.3] that gives the un-normalized eigenvalues

$$\theta_j = q^{j+1} \begin{bmatrix} d_1 - j \\ 1 \end{bmatrix} \begin{bmatrix} n - d_1 - j \\ 1 \end{bmatrix} - \begin{bmatrix} j \\ 1 \end{bmatrix}$$

and the degree is

$$k = q \begin{bmatrix} d_1 \\ 1 \end{bmatrix} \begin{bmatrix} n - d_1 \\ 1 \end{bmatrix}$$

Plugging in $j = 1$ one gets the second largest eigenvalue in absolute value is approximately

$$\lambda(Gr(m, d_1)) \approx \frac{1}{\sqrt{q}}. \tag{3}$$

It can be shown that $\lambda(\mathcal{I}_{d_1,d_2}(0)) \approx (\lambda(Gr(m,d_1)))^{d_2-d_1}$. When adding W we are essentially moving to the graph $\mathcal{I}_{d_1,d_2-d_0}(0)$, i.e. $\lambda(\mathcal{I}_{d_1,d_2}(d_0)) \approx \lambda(\mathcal{I}_{d_1,d_2-d_0}(0))$. ◀

We shall use the following sampling property of $\mathcal{I}_{d_1,d_2}(d_0)$.

▶ **Proposition 11.** *Let $G = (L \cup R, E)$ be a bipartite graph with second largest normalized singular value λ. Then for any subset $A \subseteq L$ of density α it holds that $|N(A)| \geq (1-\lambda^2/\alpha)\cdot|R|$ where $N(A)$ denotes the set of neighbors of A in R.*

Proof. Let $B := R \setminus N(A)$ and $\beta := |B|/|R|$. Noting that $\Pr_{(u,v)\in E}[u \in A \wedge v \in B] = 0$, by expander mixing lemma (see e.g., [13, Lemma 2.8.]) we have that

$$\alpha\beta = \left| \Pr_{(u,v)\in E}[u \in A \wedge v \in B] - \alpha\beta \right| \leq \lambda\sqrt{\alpha\beta},$$

and so $\beta \leq \lambda^2/\alpha$. It follows that $|N(A)| = (1-\beta)|R| \geq (1-\lambda^2/\alpha)|R|$. ◀

4 From agreement testing to robust testing

In this section we prove the following lemma showing the agreement testing to robust testing implication.

▶ **Lemma 12** (Agreement testing implies robust testing). *Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq s > t \geq \ell$. Suppose that $C^{\ell \nearrow m}$ is (s, t, α)-agreement testable, and let $\delta := \mathrm{dist}(C^{\ell \nearrow t})$. Then $C^{\ell \nearrow m}$ is $\big(s, \Omega(\alpha\delta)\big)$-robust.*

Proof. For simplicity of notation, in what follows we let T, S denote the random variables obtained by sampling a uniform random affine subspace of dimension t, s respectively. Suppose that $f : \mathbb{F}_q^m \to \mathbb{F}_q$ has $\mathbb{E}_S[\mathrm{dist}(f|_S, C^{\ell \nearrow s})] \leq \epsilon$, our goal is to find a codeword $g \in C^{\ell \nearrow m}$ such that $\mathrm{dist}(f, g) \leq O(\epsilon/(\alpha\delta))$.

The proof proceeds as follows. We would like to apply our assumption on agreement testability, and towards this, we create an instance $(f_S)_S$ for the agreement tester by letting f_S be the codeword in $C^{\ell \nearrow s}$ that is closest to $f|_S$. We then use the fact that f_S is typically close to $f|_S$, together with the fact that t-dimensional affine subspaces sample well inside s-dimensional affine subspaces, and the assumption that C has distance on t-dimensional affine subspaces, to show that $\Pr_{T,\, S \supseteq T,\, S' \supseteq T}[f_S|_T \neq f_{S'}|_T]$ is small. Agreement testability then gives a codeword $g \in C^{\ell \nearrow m}$ that is consistent with most f_S, and using the fact that s-dimensional affine subspaces sample well inside $\mathbb{F}_q^m$ this implies in turn that $\mathrm{dist}(f, g)$ is small. Details follow.

We begin by showing that $\Pr_{T,\, S \supseteq T,\, S' \supseteq T}[f_S|_T \neq f_{S'}|_T]$ is small. Recall first that $\mathbb{E}_S[\mathrm{dist}(f|_S, f_S)] = \mathbb{E}_S[\mathrm{dist}(f|_S, C^{\ell \nearrow s})] \leq \epsilon$. Next observe that for a fixed s-dimensional affine subspace S, any point in a uniform random t-dimensional affine subspace contained in S is uniform in S. Thus we also have that $\mathbb{E}_{S,\, T \subseteq S}[\mathrm{dist}(f|_T, f_S|_T)] \leq \epsilon$, and consequently

$$\begin{aligned}
\Pr_{T,\, S \supseteq T,\, S' \supseteq T}\big[\mathrm{dist}(f_S|_T, f_{S'}|_T) \geq \delta\big] &\leq 2 \cdot \Pr_{T,\, S \supseteq T}\big[\mathrm{dist}(f|_T, f_S|_T) \geq \delta/2\big] \\
&= 2 \cdot \Pr_{S,\, T \subseteq S}\big[\mathrm{dist}(f|_T, f_S|_T) \geq \delta/2\big] \\
&\leq \frac{4\epsilon}{\delta}.
\end{aligned}$$

But since $f_S|_T$, $f_{S'}|_T$ are both codewords of $C^{\ell \nearrow t}$, a code of relative distance δ, the above implies in turn that $\Pr_{T,\, S \supseteq T,\, S' \supseteq T}[f_S|_T \neq f_{S'}|_T] \leq \frac{4\epsilon}{\delta}$.

Our assumption on agreement testability now gives a codeword $g \in C^{\ell \nearrow m}$ that has $\Pr_S[g|_S \neq f_S] \leq 4\epsilon/(\alpha\delta)$. But since any point in a uniform random s-dimensional affine subspace is uniform in $\mathbb{F}_q^m$ this gives in turn that

$$\mathrm{dist}(f, g) = \mathbb{E}_S\big[\mathrm{dist}(f|_S, g|_S)\big] \leq \mathbb{E}_S\big[\mathrm{dist}(f|_S, f_S)\big] + \mathbb{E}_S\big[\mathrm{dist}(f_S, g|_S)\big] \leq \epsilon + \frac{4\epsilon}{\alpha\delta} \leq \frac{5\epsilon}{\alpha\delta}. \quad \blacktriangleleft$$

5 From local testing to agreement testing

In this section we prove the following lemma that gives the local testing to agreement testing implication.

▶ **Lemma 13** (Local testing implies agreement testing). *Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq k \geq \ell$. Suppose that $C^{\ell \nearrow m}$ is (k, α)-testable, and let $\delta := \min_{k \leq r \leq m} \mathrm{dist}(C^{\ell \nearrow r})$. Then $C^{\ell \nearrow m}$ is $(2k + \log_q(4/\delta), k + 1, \Omega(\alpha \cdot \delta^2))$-agreement testable.*

Proof outline

For simplicity of notation, in what follows let $s := 2k + \log_q(4/\delta)$ and $t := k + 1$. We let both S, S' (T, T' and K, K', resp.) denote random variables obtained by sampling a uniform random affine subspace of dimension s (t, k, resp.).

Let $(f_S)_S$ be a collection of partial assignments such that $f_S \in C^{\ell \nearrow s}$ for every S, and

$$\Pr_{T,\, S \supseteq T,\, S' \supseteq T}[f_S|_T \neq f_{S'}|_T] \leq \epsilon. \tag{4}$$

Our goal is to find a global codeword $g \in C^{\ell \nearrow m}$ that has

$$\Pr_S[g|_S \neq f_S] \leq O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right). \tag{5}$$

We find the codeword g in three stages.

1. In the initial stage (Section 5.1) we define for any k-dimensional affine subspace K a "most popular function" $\mathrm{Plur}_K : \mathbb{F}_q^k \to \mathbb{F}_q$ by choosing the most common value among $f_S|_K$ going over all $S \supseteq K$. We show that for a typical K, this function is obtained with an overwhelming plurality of $1 - O(\epsilon)$.
2. In the "local structure" stage (Section 5.2) we define for any k-dimensional affine subspace K a function $g_K : \mathbb{F}_q^m \to \mathbb{F}_q$ by letting $g_K(x)$ be the most common "vote" among all f_S that contain both K and x and agree with Plur_K on K. We then show that for a typical K, g_K is close to some codeword $h_K \in C^{\ell \nearrow m}$, and moreover $h_K|_S = f_S$ for most S containing K.
3. In the "global structure" stage (Section 5.3) we show that there exists $\hat{K}$ for which $h_{\hat{K}}|_S = f_S$ for most S (not necessarily containing $\hat{K}$). We can then set our "global function" g to be equal to $h_{\hat{K}}$.

5.1 Initial stage

For any k-dimensional affine subspace K we let $\mathrm{Plur}_K : \mathbb{F}_q^k \to \mathbb{F}_q$ denote the most common value among $f_S|_K$ for S containing K, that is,

$$\mathrm{Plur}_K := \mathrm{plurality}_{S \supseteq K}\{f_S|_K\}.$$

Next we use our assumption (4) to show that for a typical K, the function Plur_K is obtained with overwhelming plurality.

▶ **Lemma 14.**

$$\mathbb{E}_K\left[\Pr_{S \supseteq K}\left[f_S|_K \neq \mathrm{Plur}_K\right]\right] \leq 2\epsilon.$$

Proof. Since the collision probability lower bounds the probability of hitting the most common value, it suffices to show that

$$\Pr_{K,\, S \supseteq K,\, S' \supseteq K}\left[f_S|_K \neq f_{S'}|_K\right] \leq 2\epsilon. \tag{6}$$

Clearly if $t = k$ we would be done by (4), so the whole point is to show the same for $t > k$. We describe a distribution on triples (S_1, S', S_2) such that (S_1, S_2) are distributed as in (6) but the pairs (S_1, S') and (S', S_2) are distributed as in (4):

1. Choose a uniform random k-dimensional affine subspace K.
2. Choose a pair of uniform random t-dimensional affine subspaces T_1, T_2 containing K.

3. For $i = 1, 2$, choose a uniform random s-dimensional affine subspace S_i containing T_i.
4. Choose a uniform random s-dimensional affine subspace S' containing $T_1 \cup T_2$ (this can be done since $t = k + 1$ and $s \geq k + 2$).

One can check that indeed K, S_1, S_2 are distributed as in (6) while T_i, S_i, S' are distributed as in (4). Thus by our assumption (4),

$$\Pr_{K,\, S_1 \supseteq K,\, S_2 \supseteq K} \left[f_{S_1}|_K \neq f_{S_2}|_K \right]$$
$$\leq \Pr_{T_1,\, S_1 \supseteq T_1,\, S' \supseteq T_1} \left[f_{S_1}|_{T_1} \neq f_{S'}|_{T_1} \right] + \Pr_{T_2,\, S' \supseteq T_2,\, S_2 \supseteq T_2} \left[f_{S'}|_{T_2} \neq f_{S_2}|_{T_2} \right] \leq 2\epsilon. \quad \blacktriangleleft$$

5.2 Local structure

Next we define for every k-dimensional affine subspace K the function $g_K : \mathbb{F}_q^m \to \mathbb{F}_q$. As described above, for every $x \in \mathbb{F}_q^m$, we let $g_K(x)$ be the most common value among $f_S(x)$ for S that contain both K and x and agree with Plur_K on K, that is,

$$g_K(x) := \mathrm{plurality}_{S \supseteq K \cup \{x\},\, f_S|_K = \mathrm{Plur}_K} \{f_S(x)\}.$$

Next we would like to show that for a typical K, g_K is close to some codeword $h_K \in C^{\ell \nearrow m}$, and additionally $h_K|_S = f_S$ for most S containing K. We show these in three steps:

1. Boosting step (Lemma 15): In this step we show that for typical K, x, the plurality in the definition of $g_K(x)$ is obtained with overwhelming probability.
2. LTC step (Lemma 16): In this step we use the previous step to show that for a typical g_K, for most K', $g_K|_{K'}$ agrees with some f_S on K', and therefore is a codeword of $C^{\ell \nearrow k}$. By local testability assumption this implies in turn that such g_K is close to being in the code $C^{\ell \nearrow m}$, and we denote by $h_K \in C^{\ell \nearrow m}$ the closest codeword to g_K.
3. Agreement step (Lemma 17): In this step we show that a typical h_K agrees with most f_S for $S \supseteq K$.

We start with the boosting step, showing that for typical K, x, the plurality in the definition of $g_K(x)$ is obtained with overwhelming probability. Intuitively, this follows by assumption that the code has distance on t-dimensional affine subspaces, together with the fact that k-dimensional affine subspaces sample well inside t-dimensional affine subspaces, which imply that if a pair of f_S agree on K then they must typically also agree on their whole intersection.

▶ **Lemma 15** (Boosting step).

$$\mathbb{E}_{K,\, x \notin K} \left[\Pr_{S \supseteq K \cup \{x\}} \left[f_S(x) \neq g_K(x) \mid f_S|_K = \mathrm{Plur}_K \right] \right] \leq O\left(q^{-k} \cdot \frac{\epsilon}{\delta \cdot (1 - 4\epsilon)} \right).$$

Proof. Since the collision probability lower bounds the probability of hitting the most common value, it suffices to show that

$$\Pr_{K,\, x \notin K,\, S \supseteq K \cup \{x\},\, S' \supseteq K \cup \{x\}} \left[f_S(x) \neq f_{S'}(x) \mid f_S|_K = f_{S'}|_K = \mathrm{Plur}_K \right] \leq O\left(q^{-k} \cdot \frac{\epsilon}{\delta \cdot (1 - 4\epsilon)} \right).$$

Now we have that

$$\Pr_{K,\, x \notin K,\, S \supseteq K \cup \{x\},\, S' \supseteq K \cup \{x\}} \left[f_S(x) \neq f_{S'}(x) \mid f_S|_K = f_{S'}|_K = \mathrm{Plur}_K \right]$$
$$\leq \Pr_{K,\, T \supseteq K,\, S \supseteq T,\, S' \supseteq T} \left[f_S|_T \neq f_{S'}|_T \mid f_S|_K = f_{S'}|_K = \mathrm{Plur}_K \right]$$
$$= \frac{\Pr_{T,\, S \supseteq T,\, S' \supseteq T,\, K \subseteq T} \left[f_S|_K = f_{S'}|_K = \mathrm{Plur}_K \mid f_S|_T \neq f_{S'}|_T \right] \cdot \Pr_{T,\, S \supseteq T,\, S' \supseteq T} \left[f_S|_T \neq f_{S'}|_T \right]}{\Pr_{K,\, T \supseteq K,\, S \supseteq T,\, S' \supseteq T} \left[f_S|_K = f_{S'}|_K = \mathrm{Plur}_K \right]}.$$

Next we bound each of the terms above.

By our assumption (4), the right hand term in the numerator is upper bounded by ϵ. To bound the denominator note that by Lemma 14,

$$\Pr_{K,\, T\supseteq K,\, S\supseteq T,\, S'\supseteq T}[f_S|_K = f_{S'}|_K = \mathrm{Plur}_K] \geq 1 - 2\cdot \Pr_{K,\, S\supseteq K}[f_S|_K \neq \mathrm{Plur}_K] \geq 1 - 4\epsilon. \quad (7)$$

To bound the left hand term in the numerator note first that since $f_S, f_{S'}$ are both codewords of $C^{\ell\nearrow s}$ then $f_S|_T, f_{S'}|_T$ are distinct codewords in $C^{\ell\nearrow t}$, and so $\mathrm{dist}(f_S|_T, f_{S'}|_T) \geq \delta$. We now apply Propositions 10 and 11 on the graph $\mathcal{I}_{0,k}(0)$: The ambient space is T, and the graph connects the points of T (which are the 0-dimensional affine subspaces contained in T) on the left to the k-dimensional affine subspaces contained in T on the right. By Proposition 10 the graph $\mathcal{I}_{0,k}(0)$ has second largest normalized singular value at most $q^{-k/2}$, and so taking $A = \{x \in T \mid \ f_S(x) \neq f_{S'}(x)\}$ in Proposition 11 we deduce that at most q^{-k}/δ fraction of K can miss A altogether. Thus,

$$\Pr_{T,\, S\supseteq T,\, S'\supseteq T,\, K\subseteq T}\left[f_S|_K = f_{S'}|_K \;\middle|\; f_S|_T \neq f_{S'}|_T\right] \leq \frac{q^{-k}}{\delta}. \quad (8)$$

The final bound is obtained by combining the bounds in (4), (7), and (8). ◀

Next we use the assumption on local testability to show that for a typical K, g_K is close to being a codeword of $C^{\ell\nearrow m}$.

▶ **Lemma 16** (LTC step)**.**

$$\mathbb{E}_K\left[\mathrm{dist}\big(g_K, C^{\ell\nearrow m}\big)\right] \leq O\left(\frac{\epsilon}{\alpha\cdot\delta}\right).$$

Proof. To apply our assumption on local testability we first show that $g_K|_{K'}$ is typically a codeword of $C^{\ell\nearrow k}$. For this, first observe that if $g_K|_{K'}$ is not a codeword of $C^{\ell\nearrow k}$ then $g_K|_{K'} \neq f_S|_{K'}$ for all S (since $f_S \in C^{\ell\nearrow s}$ and so $f_S|_{K'} \in C^{\ell\nearrow k}$). Thus we have

$$\mathbb{E}_{K,\, K'}\left[\mathbb{1}_{g_K|_{K'}\notin C^{\ell\nearrow k}}\right] \leq \mathbb{E}_{K,\, K'}\left[\Pr_{S\supseteq K\cup K'}[g_K|_{K'} \neq f_S|_{K'}]\right]$$

$$\leq \mathbb{E}_{K,\, K'}\left[\Pr_{S\supseteq K\cup K'}\left[g_K|_{K'} \neq f_S|_{K'} \;\middle|\; f_S|_K = \mathrm{Plur}_K\right]\right] + \Pr_{K,\, S\supseteq K}[f_S|_K \neq \mathrm{Plur}_K]$$

We claim that the above expression is at most $O(\epsilon/\delta)$. To see this note first that by Lemma 14 the right hand term is at most 2ϵ . To bound the left hand term, note that since each individual point in K' is uniformly distributed in $\mathbb{F}_q^m$ this term is upper bounded by

$$q^k \cdot \mathbb{E}_{K,\, x}\left[\Pr_{S\supseteq K\cup\{x\}}\left[g_K(x) \neq f_S(x) \;\middle|\; f_S|_K = \mathrm{Plur}_K\right]\right],$$

which is in turn at most $O(\epsilon/\delta)$ by Lemma 15 (noting that the probability in the above expression is zero whenever $x \in K$).

Finally, for any k-dimensional affine subspace K let $\epsilon_K := \Pr_{K'}\left[g_K|_{K'} \notin C^{\ell\nearrow k}\right]$. Then on the one hand $\mathbb{E}_K[\epsilon_K] = \mathbb{E}_{K,\, K'}\left[\mathbb{1}_{g_K|_{K'}\notin C^{\ell\nearrow k}}\right] \leq O(\epsilon/\delta)$, and on the other hand $\mathrm{dist}(g_K, C^{\ell\nearrow m}) \leq \epsilon_K/\alpha$ for any K by assumption that $C^{\ell\nearrow m}$ is (k,α)-testable. We conclude that

$$\mathbb{E}_K\left[\mathrm{dist}\big(g_K, C^{\ell\nearrow m}\big)\right] \leq \mathbb{E}_K\left[\frac{\epsilon_K}{\alpha}\right] \leq O\left(\frac{\epsilon}{\alpha\cdot\delta}\right).$$ ◀

For any k-dimensional affine subspace K let $h_K \in C^{\ell \nearrow m}$ be the codeword that is closest to g_K. Then by the above lemma,

$$\mathbb{E}_K \left[\operatorname{dist}(g_K, h_K)\right] \leq O\left(\frac{\epsilon}{\alpha \cdot \delta}\right).$$

The following lemma says that for a typical K we have that $h_K|_S = f_S$ for most S containing K, which follows by the fact that s-dimensional affine subspaces sample well inside $\mathbb{F}_q^m$ and by assumption that the code has distance on s-dimensional affine subspaces.

▶ **Lemma 17** (Agreement step)**.**

$$\mathbb{E}_K \left[\Pr_{S \supseteq K} \left[h_K|_S \neq f_S\right]\right] \leq O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right).$$

Proof. We show that for typical $S \supseteq K$, on the one hand, by Lemma 16 and the fact that s-dimensional affine subspaces sample well inside $\mathbb{F}_q^m$, $\operatorname{dist}(h_K|_S, g_K|_S)$ is small, and on the other hand, by Lemma 15, $\operatorname{dist}(g_K|_S, f_S)$ is small. We then conclude by triangle inequality that $\operatorname{dist}(h_K|_S, f_S)$ is small, which implies in turn that $h_K|_S = f_S$ by assumption that the code has distance on s-dimensional subspaces.

We start by showing that $\operatorname{dist}(h_K|_S, g_K|_S)$ is typically small. For this note that for a fixed k-dimensional affine subspace K and uniform random S containing K, each individual point in $S \setminus K$ is uniformly distributed in $\mathbb{F}_q^m \setminus K$. Thus we have

$$\mathbb{E}_{K,\, S \supseteq K} \left[\operatorname{dist}(h_K|_S, g_K|_S)\right] \leq q^{-(s-k)} + \mathbb{E}_K \left[\operatorname{dist}(h_K, g_K)\right] \leq \frac{\delta}{4} + O\left(\frac{\epsilon}{\alpha \cdot \delta}\right), \tag{9}$$

where the last inequality follows by choice of $s \geq k + \log_q(4/\delta)$ and Lemma 16.

Next we show that $\operatorname{dist}(h_K|_S, f_S)$ is typically small. For this note that

$$\begin{aligned}
&\mathbb{E}_{K,\, S \supseteq K} \left[\operatorname{dist}(g_K|_S, f_S)\right] \\
&\leq q^{-(s-k)} + \mathbb{E}_{K,\, x \notin K} \left[\Pr_{S \supseteq K \cup \{x\}} \left[g_K(x) \neq f_S(x)\right]\right] \\
&\leq q^{-(s-k)} + \mathbb{E}_{K,\, x \notin K} \left[\Pr_{S \supseteq K \cup \{x\}} \left[g_K(x) \neq f_S(x) \;\middle|\; f_S|_K = \operatorname{Plur}_K\right]\right] + \Pr_{K,\, S \supseteq K} \left[f_S|_K \neq \operatorname{Plur}_K\right] \\
&\leq \frac{\delta}{4} + O\left(\frac{\epsilon}{\delta}\right),
\end{aligned} \tag{10}$$

where the last inequality follows by choice of $s \geq k + \log_q(4/\delta)$ and Lemmas 15 and 14.

Combining (9) and (10), by triangle inequality we have that

$$\mathbb{E}_{K,\, S \supseteq K} \left[\operatorname{dist}(h_K|_S, f_S)\right] \leq \frac{\delta}{2} + O\left(\frac{\epsilon}{\alpha \cdot \delta}\right),$$

and by Markov's inequality,

$$\Pr_{K,\, S \supseteq K} \left[\operatorname{dist}(h_K|_S, f_S) \geq \delta\right] \leq O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right).$$

Finally, since both $h_K|_S$ and f_S are codewords of $C^{\ell \nearrow s}$ and $\operatorname{dist}(C^{\ell \nearrow s}) \geq \delta$ we conclude that $h_K|_S \neq f_S$ with probability at most $O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right)$ over the choice of K and $S \supseteq K$. ◀

5.3 Global structure

We now complete the proof of Lemma 13 by showing that there exists a codeword $g \in C^{\ell \nearrow m}$ that agrees with most f_S. We start by showing that most functions h_K are in fact identical, which follows by Lemma 17 and the fact that s-dimensional affine subspaces sample well inside $\mathbb{F}_q^m$.

▶ **Lemma 18.** *There exists a k-dimensional affine subspace $\hat{K}$ such that*

$$\Pr_K \left[h_K \neq h_{\hat{K}}\right] \leq O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right).$$

Proof. By Lemma 17,

$$\Pr_{K,\, K',\, S \supseteq K \cup K'} \left[h_K|_S \neq h_{K'}|_S\right] \leq 2 \cdot \Pr_{K,\, S \supseteq K} \left[h_K|_S \neq f_S\right] \leq O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right),$$

and so by averaging there exists $\hat{K}$ such that

$$\Pr_{K,\, S \supseteq K \cup \hat{K}} \left[h_K|_S \neq h_{\hat{K}}|_S\right] \leq O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right).$$

Markov's inequality then implies that

$$\Pr_{S \supseteq K \cup \hat{K}} \left[h_K|_S \neq h_{\hat{K}}|_S\right] \geq \frac{1}{2}$$

with probability at most $O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right)$ over the choice of K.

Next observe that if $h_K \neq h_{\hat{K}}$ then since h_K, $h_{\hat{K}}$ are both codewords of $C^{\ell \nearrow m}$ and $\mathrm{dist}(C^{\ell \nearrow m}) \geq \delta$, it must hold that $\mathrm{dist}(h_K, h_{\hat{K}}) \geq \delta$. We now apply Propositions 10 and 11 on the graph $\mathcal{I}_{0,s}(2k)$ that connects the points of $\mathbb{F}_q^m$ on the left to the s-dimensional affine subspaces containing $K \cup \hat{K}$ on the right. By Proposition 10 the graph $\mathcal{I}_{0,s}(2k)$ has second largest normalized singular value at most $q^{-(s-2k)/2}$, and so taking $A = \left\{x \in \mathbb{F}_q^m \;\middle|\; h_K(x) \neq h_{\hat{K}}(x)\right\}$ in Proposition 11 we deduce that

$$\Pr_{S \supseteq \hat{K} \cup K} \left[h_{\hat{K}}|_S \neq h_K|_S\right] \geq 1 - \frac{q^{-(s-2k)}}{\delta} \geq 1/2,$$

where the last inequality follows by assumption that $s \geq 2k + \log_q(2/\delta)$.

It now follows that $h_K \neq h_{\hat{K}}$ with probability at most $O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right)$ over the choice of K. ◀

We can now complete the proof of Lemma 13.

Proof of Lemma 13. Set $g \in C^{\ell \nearrow m}$ to be the function $h_{\hat{K}}$ guaranteed by Lemma 18. By Lemmas 17 and 18,

$$\Pr_S \left[g|_S \neq f_S\right] = \Pr_{K,\, S \supseteq K} \left[g|_S \neq f_S\right] \leq \Pr_K \left[g \neq h_K\right] + \Pr_{K,\, S \supseteq K} \left[h_K|_S \neq f_S\right] \leq O\left(\frac{\epsilon}{\alpha \cdot \delta^2}\right).$$

So g satisfies (5) as required. ◀

6 From local testing to robust testing

6.1 Proof of Main Theorem 1

We can now combine Lemmas 12 and 13 to prove our main Theorem 1, showing a transformation from local testing to robust testing.

Proof of Theorem 1. By Lemma 13 we have that $C^{\ell \nearrow m}$ is $(2k + \log_q(4/\delta), k+1, \Omega(\alpha \cdot \delta^2))$-agreement testable, and by Lemma 12 this implies in turn that $C^{\ell \nearrow m}$ is $(2k + \log_q(4/\delta), \Omega(\alpha \cdot \delta^3))$-robust. ◀

6.2 Proof of Corollary 2

We now instantiate our main Theorem 1 with Theorem 6 to show that lifted codes are robustly testable. For this, we first observe that one can amplify the soundness of the tester given by Theorem 6 to a constant (independent of q and ℓ) at the cost of increasing the testing dimension to $\approx 3\ell$.

▶ **Proposition 19.** *Let $C \subseteq \{\mathbb{F}_q^\ell \to \mathbb{F}_q\}$ be an affine-invariant linear code, and $m \geq 3\ell + \log_q 4$. Then $C^{\ell \nearrow m}$ is $\big(3\ell + \log_q 4, \Omega(1)\big)$-testable.*

Proof. If the ℓ-dimensional test rejects with probability at least $\frac{1}{2} \cdot \mathrm{dist}(f, C^{\ell \nearrow m})$ then by Part (3) of Proposition 8, the $(3\ell + \log_q 4)$-dimensional test also rejects with the same probability and we are done. Otherwise, by Theorem 6, the ℓ-dimensional test rejects with probability at least $\frac{1}{2} \cdot q^{-2\ell}$.

Consider the graph $\mathcal{I}_{\ell,3\ell+\log_q 4}(0)$ with left hand side being all ℓ-dimensional affine subspaces of $\mathbb{F}_q^m$ and right hand side being all $(3\ell + \log_q 4)$-dimensional affine subspaces of $\mathbb{F}_q^m$. Next we apply Propositions 10 and 11 on the graph $\mathcal{I}_{\ell,3\ell+\log_q 4}(0)$ with A being the collection of all ℓ-dimensional affine subspaces on which the ℓ-dimensional test rejects. Noting that the $(3\ell + \log_q 4)$-dimensional test will reject on any neighbor of A we conclude that the $(3\ell + \log_q 4)$-dimensional test rejects with probability at least $1 - \frac{q^{-(2\ell+\log_q 4)}}{q^{-2\ell}/2} = \frac{1}{2}$. ◀

We now turn to the proof of Corollary 2.

Proof of Corollary 2. Suppose first that $\delta < 2q^{-\ell}$. In this case by Theorem 6, $C^{\ell \nearrow m}$ is $(\ell, \Omega(q^{-2\ell}))$-testable, and so by Part (2) of Prposition 8, $C^{\ell \nearrow m}$ is also robustly testable using the ℓ-dimensional test with robustness $\Omega\big(q^{-3\ell}\big) \geq \Omega(\delta^3)$. By Part (4) of Proposition 8 it follows that the $(6\ell + \log_q(128/\delta))$-dimensional test also has robustness $\Omega(\delta^3)$.

Next assume that $\delta \geq 2q^{-\ell}$. In this case Proposition 4 gives that $\mathrm{dist}(C^{\ell \nearrow r}) \geq \delta/2$ for any $\ell \leq r \leq m$, and so we may apply Proposition 19 and Theorem 1 and conclude that $C^{\ell \nearrow m}$ is $(6\ell + \log_q(128/\delta), \Omega(\delta^3))$-robust. ◀

References

1. Sanjeev Arora. *Probabilistic checking of proofs and hardness of approximation problems.* PhD thesis, Princeton University, 1994.
2. Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, May 1998.
3. Sanjeev Arora and Shmuel Safra. Probabilistic Checking of Proofs: A New Characterization of NP. *Journal of the ACM*, 45(1):70–122, January 1998.
4. Sanjeev Arora and Madhu Sudan. Improved Low Degree Testing and its Applications. *Combinatorica*, 23(3):365–426, 2003.
5. Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil P. Vadhan. Robust PCPs of Proximity, Shorter PCPs, and Applications to Coding. *SIAM J. Comput*, 36(4):889–974, 2006.
6. Eli Ben-Sasson, Prahladh Harsha, and Sofya Raskhodnikova. Some 3CNF Properties Are Hard to Test. *SICOMP: SIAM Journal on Computing*, 35, 2005.
7. Eli Ben-Sasson, Ghid Maatouk, Amir Shpilka, and Madhu Sudan. Symmetric LDPC Codes are not Necessarily Locally Testable. In *IEEE Conference on Computational Complexity*, pages 55–65. IEEE Computer Society, 2011. doi:10.1109/CCC.2011.14.
8. Eli Ben-Sasson and Madhu Sudan. Robust locally testable codes and products of codes. *Random Struct. Algorithms*, 28(4):387–402, 2006. doi:10.1002/rsa.20120.

9 Eli Ben-Sasson and Michael Viderman. Composition of semi-LTCs by two-wise tensor products. *Computational Complexity*, 24(3):601–643, 2015. doi:10.1007/s00037-013-0074-8.

10 Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-Testing/Correcting with Applications to Numerical Problems. In *STOC*, pages 73–83. ACM, 1990.

11 A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Springer Verlag, 1989.

12 Irit Dinur and Elazar Goldenberg. Locally Testing Direct Product in the Low Error Range. In *FOCS*, pages 613–622. IEEE Computer Society, 2008. doi:10.1109/FOCS.2008.26.

13 Irit Dinur and Tali Kaufman. High Dimensional Expanders Imply Agreement Expanders. In Chris Umans, editor, *FOCS*, pages 974–985. IEEE Computer Society, 2017. doi:10.1109/FOCS.2017.94.

14 Irit Dinur and Inbal Livni-Navon. Exponentially Small Soundness for the Direct Product Z-Test. In Ryan O'Donnell, editor, *Computational Complexity Conference*, volume 79 of *LIPIcs*, pages 29:1–29:50. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017. doi:10.4230/LIPIcs.CCC.2017.29.

15 Irit Dinur and Omer Reingold. Assignment Testers: Towards a Combinatorial Proof of the PCP Theorem. *SIAM J. Comput*, 36(4):975–1024, 2006. doi:10.1137/S0097539705446962.

16 Irit Dinur and David Steurer. Direct Product Testing. In *IEEE Conference on Computational Complexity*, pages 188–196. IEEE Computer Society, 2014. doi:10.1109/CCC.2014.27.

17 Peter Gemmell, Richard J. Lipton, Ronitt Rubinfeld, Madhu Sudan, and Avi Wigderson. Self-Testing/Correcting for Polynomials and for Approximate Functions. In Cris Koutsougeras and Jeffrey Scott Vitter, editors, *STOC*, pages 32–42. ACM, 1991. doi:10.1145/103418.103429.

18 Goldreich and Safra. A Combinatorial Consistency Lemma with Application to Proving the PCP Theorem. *SICOMP: SIAM Journal on Computing*, 29, 1999.

19 Alan Guo, Elad Haramaty, and Madhu Sudan. Robust Testing of Lifted Codes with Applications to Low-Degree Testing. In Venkatesan Guruswami, editor, *FOCS*, pages 825–844. IEEE Computer Society, 2015. doi:10.1109/FOCS.2015.56.

20 Alan Guo, Swastik Kopparty, and Madhu Sudan. New affine-invariant codes from lifting. In *ITCS*, pages 529–540, 2013.

21 Elad Haramaty, Noga Ron-Zewi, and Madhu Sudan. Absolutely Sound Testing of Lifted Codes. *Theory of Computing*, 11:299–338, 2015. doi:10.4086/toc.2015.v011a012.

22 Russell Impagliazzo, Valentine Kabanets, and Avi Wigderson. New Direct-Product Testers and 2-Query PCPs. *SIAM J. Comput*, 41(6):1722–1768, 2012. doi:10.1137/09077299X.

23 Tali Kaufman and Madhu Sudan. Algebraic property testing: the role of invariance. In *STOC*, pages 403–412. ACM, 2008. doi:10.1145/1374376.1374434.

24 Swastik Kopparty, Or Meir, Noga Ron-Zewi, and Shubhangi Saraf. High-Rate Locally Correctable and Locally Testable Codes with Sub-Polynomial Query Complexity. *Journal of ACM*, 64(2):11:1–11:42, 2017. doi:10.1145/3051093.

25 Ran Raz and Shmuel Safra. A Sub-Constant Error-Probability Low-Degree Test, and a Sub-Constant Error-Probability PCP Characterization of NP. In *STOC*, pages 475–484. ACM, 1997. doi:10.1145/258533.258641.

26 Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM Journal on Computing*, 25(2):252–271, April 1996.

27 Michael Viderman. A combination of testability and decodability by tensor products. *Random Struct. Algorithms*, 46(3):572–598, 2015.